STATE OF VERMONT
Agency of Human Services (AHS)

Incident Response	REVISION HISTORY:	Chapter/Number 5.05
	EFFECTIVE DATE:	Attachments/Related Documents:

Authorizing Signature: Cynthia D. LaWare Date Signed: 11/12/08

Cynthia LaWare, Secretary, Agency of Human Services

PURPOSE

To ensure effective monitoring and response to all Information Technology (IT) incidents or suspected incidents by addressing all critical aspects of Incident Response (IR) and containment.

BACKGROUND and REFERENCES:

NIST Special Publication 800-61, Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

45 CFR 164.308(a)(6) Health Insurance Portability and Accountability Act (1996), Security Incident Procedures Standard

DEFINITIONS:

CSIRT- Computer Security Incident Response Team

Event- an observable occurrence within a system or network

Security Incident- a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

Reportable Security Incident- attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; or interference with system operations in an information system

SCOPE:

This document applies to all Agency Departments, Divisions and Offices hereafter referred to jointly as "department". This document also applies to contractors, business associates, and other users of departmental information systems.

STANDARDS:

AHS employees shall be responsible for communicating reportable security incidents to the AHS Incident Response team.

The AHS Information Systems Security Director shall establish an Agency CSIRT team. The team, working with departmental IT Managers, shall develop, disseminate, review, and update AHS CSIRT controls. The team will also develop, document, and implement procedures to effectively monitor and respond to all IT security incidents or suspected incidents by addressing all critical aspects of incident

handling and response containment. The Incident Response (IR) procedures shall be consistent with applicable laws, directives, policies, regulations, standards, and guidance.

As a result of this policy, plans and procedures shall ensure the following:

- Training of employees and IT personnel in their IR roles and responsibilities with respect to AHS information systems.
- Periodic documented testing of IR capability for AHS information systems to determine the plan's effectiveness.
- Incident handling capability including preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to security incidents.
- Preservation of evidence of computer crimes, computer misuse, and all other unlawful computer activities.
- Ongoing monitoring of AHS information systems.
- Ongoing tracking and documentation of all reported security incidents.
- Reporting of all IT systems incidents, or suspected incidents to the designated AHS CSIRT and state CSIRT.

COMPLIANCE:

It is the responsibility of the individual departments to ensure dissemination and review of this policy to all employees within their organizations and other associates as appropriate.

ENFORCEMENT:

The Office of the Secretary may initiate reviews, assessments or other means to ensure that policies, guidelines or standards are being followed.